Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short Range Communications Service in the 5.850-5.925 GHz Band	)	RM-11771

Opposition to Petition for Rulemaking and Request for Emergency Stay
of the Information Technology and Innovation Foundation

INTRODUCTION AND SUMMARY

The Information Technology and Innovation Foundation (ITIF)[1] respectfully submits this statement in opposition to the above-captioned Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short-Range Communications Service (DSRC).[2]

Filed by Public Knowledge and the Open Technology Institute at New America, the petition requests extreme measures by the Federal Communication Commission (FCC). Specifically, the petition requests an emergency prohibition of DSRC operations in the 5.9 GHz band until the FCC develops cybersecurity and privacy regulations specific to a single technology—DSRC.[3]

---

[1] Founded in 2006, The Information Technology and Innovation Foundation, or ITIF, is a 501(c)(3) nonprofit, nonpartisan research and educational institute—a think tank—focusing on a host of critical issues at the intersection of technological innovation and public policy. Its mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

[2] Public Knowledge and Open Technology Institute, "Petition for Rulemaking and Request for Emergency Stay of Operation of Dedicated Short Range Communications Service in the 5.850-5.925 GHz Band," CG RM-11771 (July 28, 2016) *available at* https://ecfsapi.fcc.gov/file/10628707126715/DSRC%20Petition%20FINAL.pdf.

[3] Id.

Reserving comment on ongoing discussion of DSRC and WiFi sharing in the 5.9 GHz band, ITIF opposes the petition. The FCC should not police what innovations are allowed to be deployed based on hypothetical privacy concerns. While ITIF believes the specific fears articulated in the petition are spurious, staying operations of otherwise compliant technology—even based on more legitimate privacy or security concerns—would be bad policy. The requested stay would be an extraordinary and likely unlawful expansion of the FCC's authority with serious detrimental effects on innovation.

What is worse, the petition requests the FCC initiate a rulemaking to expand its Customer Proprietary Network Information (CPNI) rules to a non-common carrier, even though the petition acknowledges the fact that "DSRC is not a Title II Service, nor would the Commission's CPNI regulations precisely fit the information that DSRC licensees contemplate collecting."[4]

CPNI rules were intended to address information gathered by common carriers (originally basic landline telephone networks)—such as phone numbers, consumers' history of purchases, and the frequency, duration, and timing of calls. This proposal would expand CPNI regulations far beyond their originally intended scope –telephone networks—and even beyond the recently proposed broadband privacy regime.[5] This would be an unnecessary and damaging expansion of the FCC's privacy jurisdiction.

ITIF opposes the petition believing that the actions proposed in the petition would be detrimental to innovation in how automakers collect and use consumer information. Not only is halting DSRC deployment for commercial applications premature, the FCC is ill-equipped to regulate privacy and security issues for the auto industry. Just like the FCC's foray into broadband privacy regulation, this issue should be best left to other regulators with a proven track record of preventing consumer harms.[6] To this end, FCC should promote permissionless innovation in connected vehicle applications and defer to the Federal Trade Commission's (FTC) regulatory model of privacy and cybersecurity enforcement.

PROMOTE PERMISSIONLESS INNOVATION IN CONNECTED VEHICLE APPLICATIONS

The precautionary principle states that policy actions which pose a severe risk to the public should be avoided unless convincing evidence can be shown that the harm will be avoided. While this principle is useful in some domains, it has repeatedly been shown to be an inappropriate framing for modern technology policy debates

---

[4] Id at 21.

[5] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 31 FCC Rcd 2500 (2016) (*Privacy NPRM*).

[6] Doug Brake, Daniel Castro, and Alan McQuinn, "Broadband Privacy: The Folly of Sector Specific Regulation," *Information Technology and Innovation Foundation*, March 2016, http://www2.itif.org/2016-broadband-privacy-folly.pdf.

because of its severe impact on innovation.[7] Granting the requested stay would be an embrace of the precautionary principle, stopping technological advancements in wireless technology in the hopes of nullifying potential harm to the public. This would obviously limit vehicle-to-vehicle (V2V) applications, but more broadly it would signal to entrepreneurs across the country that their innovations are at risk. The FCC should err on the side of encouraging experimentation and innovation instead of shutting down technologies that admittedly carry some risk based on a tenuous jurisdictional hook. Allowing new services to go forward allows risks, if real, to become concrete and addressable. Indeed, in a paper discussing potential regulations for connected cars, Adam Thierer and Ryan Hagemann at George Mason University argue that "attempting to foresee and plan for all the problems will only derail the many potential benefits associated with these technologies."[8]

The FCC should embrace the idea of "permissionless innovation," i.e. operate under the assumption that most technology is "innocent until proven guilty," which gives businesses the ability to experiment and create new products and services without being subjected to onerous regulation.[9] This strategy enabled the development of the Internet, allowing entrepreneurs to create different business models and try out new services without the prior approval of regulators.[10] By taking a hands-off approach to connected cars and not attempting to use this spectrum allocation to police privacy and cybersecurity concerns, the FCC can ensure innovation in connected vehicles proceeds apace.

THE FTC MODEL BETTER BALANCES PRIVACY AND CYBERSECURITY CONCERNS WITH INNOVATION

There is always a balance between the benefits of the use of data and the risk of privacy harms.[11] These benefits are often substantial. Consider, for example, the work of Catherine Tucker, a researcher at MIT, who has shown that the light-touch privacy regime in the United States is a significant factor in why the United

---

[7] Adam Thierer, "Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom," *Mercatus Center,* 2014, http://mercatus.org/sites/default/files/Permissionless.Innovation.web_.pdf.

[8] Adam Thierer and Ryan Hagemann, "Removing Roadblocks to Intelligent Vehicles and Driverless Cars," *Mercatus Center,* September 2014, http://mercatus.org/sites/default/files/Thierer-Intelligent-Vehicles.pdf.

[9] Thierer, "Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom."

[10] Adam Thierer, "Why Permissionless Innovation Matters," *Medium*, April 24, 2014, https://medium.com/tech-liberation/why-permissionless-innovation-matters-257e3d605b63#.nk430b94e.

[11] On this balance, see Avi Goldfarb & Catherine Tucker, "Privacy and Innovation," in Innovation Policy and the Economy, Volume 12 U. of Chicago Press (2012), 65-89.

States is leading in the Internet economy when compared to regions with more restrictive privacy regimes, such as the European Union.[12]

The body that usually supervises commercial privacy practices is, of course, the Federal Trade Commission (FTC). The FTC oversees fair competition and has broad authority under Section 5 of the Fair Trade Act to take enforcement actions against unfair or deceptive trade practices.[13] This approach focuses on avoiding consumer harm, which allows for rapid innovation and competition without assuming a particular industry direction, while protecting consumers and incentivizing industry to responsibly develop best practices. The FTC has taken actions against companies for violating their stated privacy and cybersecurity policies, and even offers specific guidance when it comes to privacy, having created a framework guided by three overarching principles: privacy by design, consumer choice, and transparency.[14]

By allowing flexibility for industry to develop best practices within these guidelines, and stepping in after the fact where problems develop, the FTC does not have to predict future technological advancements or changes in business practices. This allows firms to internalize or outsource different functions in fast-paced industries, allowing them to focus on delivering value to their customers rather than merely complying with regulations. This type of privacy and cybersecurity oversight, with rules that apply an even, light-touch approach to different actors, provides the best possible environment for dynamic competition to occur across platforms.

---

[12] Catherine Tucker, "Empirical Research on the Economic Effects of Privacy Regulation," 10 J. on Telecomm. & High Tech. L 265 (2012), http://jthtl.org/content/articles/V10I2/JTHTLv10i2_Tucker.PDF.

[13] Staff of the Bureau of Consumer Protection of the Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," *Federal Trade Commission*, March 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

[14] See, Federal Trade Commission, "Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser," news release, August 9, 2012, https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented; Federal Trade Commission, "Wyndham Settles FTC Charges It Unfairly Placed Consumers' Payment Card Information At Risk," news release, December 9, 2015, https://www.ftc.gov/news-events/press-releases/2015/12/wyndham-settles-ftc-charges-it-unfairly-placed-consumers-payment; Staff of the Bureau of Consumer Protection of the Federal Trade Commission, "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Comments of FTC Staff," at 22, WC Docket No. 16-106, available at https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumerprotection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

The FCC should, therefore, defer to the FTC's history protection of consumers' privacy and cybersecurity. It should not halt the deployment of DSRC and should not seek to expand its authority by imposing CPNI rules on automakers.

CONCLUSION

The FCC should not be cherry picking different sectors to regulate privacy or cybersecurity for any specific technology. Splintering off sector-specific rules would create a troubling problem as a wide variety of government agencies attempt to control their regulatory jurisdictions in an age of technological convergence. This problem would likely be exacerbated as the Internet of Things. Would the FCC soon start to weigh in on privacy rules for farmers adopting connected sensors on their farms? Instead of trying to pick and choose individual technologies to regulate, regulators should enforce existing consumer protection rules that allow for innovation across different sectors while still protecting consumers from harm.

There are legitimate questions over the best use of the 5.9 GHz spectrum. But those questions should be addressed directly, not through regulation of privacy and cybersecurity.

Daniel Castro
Vice President

Alan McQuinn
Research Analyst

Doug Brake
Telecommunications Policy Analyst

Information Technology and Innovation Foundation
1101 K Street NW, Suite 610
Washington, DC 20005

August 24, 2016